(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 795 264**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **99 07613**

(51) Int Cl[7] : **H 04 L 9/32**, H 04 Q 7/20

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 16.06.99.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 22.12.00 Bulletin 00/51.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *LENOIR OLIVIER* — FR et *COUR JEAN MICHEL* — FR.

(72) **Inventeur(s) :** LENOIR OLIVIER et COUR JEAN MICHEL.

(73) **Titulaire(s) :**

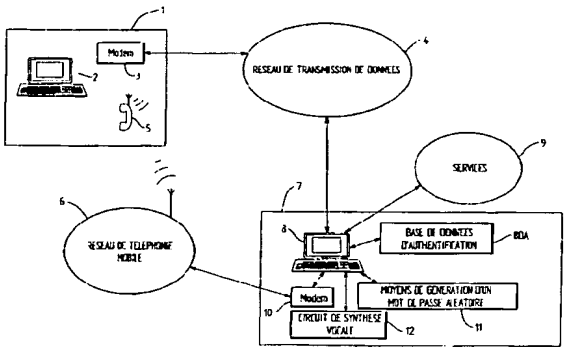
(74) **Mandataire(s) :** PONTET ET ALLANO SARL.

(54) SYSTEME ET PROCEDES D'ACCES SECURISE A UN SERVEUR INFORMATIQUE UTILISANT LEDIT SYSTEME.

(57) Le système comporte:
- un site client (1) comprenant une unité centrale de contrôle et de traitement de données (2), et un téléphone mobile (5),
- un site serveur (7) comprenant une unité centrale de commande et de traitement de données (8) prévue notamment pour gérer un protocole d'authentification du client utilisateur du site client.

Le site serveur (7) est connecté au réseau de téléphonie mobile (6) et comprend en outre: une base de données d'authentification (BDA), des moyens de synthèse vocale; et des moyens d'authentification d'un mot de passe d'authentification (MPAU) reçu par le site serveur via le réseau de transmission de données (4).

Les procédés mettant en oeuvre ce système comprennent une étape dans laquelle le serveur appelle le numéro du téléphone mobile pour demander une donnée qui est soit transmise par l'utilisateur via les touches de son téléphone mobile, soit via le réseau de transmission de données (4).



FR 2 795 264 - A1

"Système et procédés d'accès sécurisé à un serveur informatique utilisant ledit système"

La présente invention concerne un système permettant d'augmenter le niveau de sécurisation du protocole d'authentification du demandeur d'accès à un serveur informatique et deux procédés mettant en oeuvre ledit système.

Le demandeur d'accès ou client utilise en pratique un ordinateur individuel muni de moyens de connexion à un réseau de communication, par exemple le réseau Internet.

Le " serveur " est constitué d'un ordinateur muni de moyens de connexion au même réseau. Il sert à mettre en relation le client avec divers services tels que des bases de données.

La procédure d'accès au serveur pour un client se déroule classiquement en trois phases :

- l'accès au site serveur via l'établissement d'une connexion (par exemple TCP/IP), via un réseau généraliste ou privé de transmission de données (par exemple Internet) ;
- l'entrée d'une identification ; et
- l'entrée d'un mot de passe client.

L'accès est refusé si le couple [identification / mot de passe client] n'est pas conforme aux informations stockées dans une base de données dite d'"authentification " gérée par le serveur lui-même ou par un serveur intermédiaire adapté.

Les procédures connues présentent un certain nombre de faiblesses vis-à-vis de malveillances, telles que le vol des couples [code d'identification / mot de passe] via un logiciel de recherche automatique de mot de passe ou une complicité du côté " serveur " permettant de connaître le contenu de la base de données d'authentification.

Diverses solutions sont connues pour renforcer la sécurisation de l'accès :

- côté serveur un dispositif auxiliaire permettant la génération de mots de passe aléatoires et/ou cryptés, mais nécessitant la possession par le client d'un appareil synchronisé avec le serveur, générant un mot de passe pseudo-aléatoire et de courte durée de vie en fonction de la date et de l'heure ;

- la dotation des ordinateurs individuels d'un périphérique lecteur d'une carte électronique (" carte à puce "), sécurisant l'accès selon un protocole similaire à celui utilisé pour les cartes bancaires ; le client doit donc disposer d'une telle carte et d'un périphérique spécial sur le terminal à partir duquel il se connecte au réseau ;

- l'identification de la machine du client par un code d'identification tel que celui intégré par le constructeur sur ses microprocesseurs ; l'accès est sécurisé par identification du ou des composants connus du serveur ; l'inconvénient est qu'en dehors des machines dûment répertoriées, le client ne peut effectuer aucun accès.

Par ailleurs, les systèmes de cryptage connus, tels que l'algorithme RSA, nécessitent des puissances de calcul importantes pour obtenir un bon niveau de sécurité.

La présente invention a pour objet de proposer une autre solution qui soit très fiable et peu coûteuse.

Elle propose un système d'accès sécurisé à un serveur informatique, comportant:

- un site client comprenant des moyens d'accès à un réseau de transmission de données et une unité centrale de contrôle et de traitement de données ; et

- un site serveur comprenant des moyens d'accès audit réseau de transmission de données et une unité centrale de commande et de traitement de données prévue notamment pour gérer un protocole d'authentification du client utilisateur du site client,

caractérisé en ce que :

- le site client comprend en outre un téléphone mobile ; et

- le site serveur comprend en outre :

- des moyens de connexion au réseau de téléphonie mobile dudit téléphone mobile ;

- une base de données d'authentification comprenant une donnée d'identification du client et un numéro de téléphone mobile associé ;

- des moyens d'appel du numéro du téléphone mobile du client ;

- des moyens de synthèse vocale ; et

- des moyens d'authentification d'un mot de passe d'authentification reçu par le site serveur via le réseau de transmission de données.

L'idée à la base de la présente invention est donc de faire intervenir dans le protocole d'authentification un téléphone mobile, le site serveur étant muni de moyens lui permettant d'appeler le téléphone mobile et de lui transmettre un message vocal.

Le système selon l'invention n'exige du côté du site client aucun dispositif informatique spécial d'identification, intégré ou périphérique. Il requiert la possession d'un téléphone mobile ordinaire, appareil qui tend à se généraliser parmi les professionnels et les particuliers. Le coût d'équipement côté serveur reste également modeste puisque notamment un modem standard du type comportant une unité de synthèse vocale peut être utilisé pour réaliser la connexion avec le réseau de téléphonie mobile.

Un autre avantage selon l'invention réside dans le fait que ni le poste serveur, ni le poste client ne nécessitent de puissances de calcul importantes comparées aux systèmes de cryptage de l'état de la technique, d'où une forte réduction des coûts pour un système selon l'invention.

La sécurisation apportée par le système selon l'invention est renforcée par la procédure d'identification du téléphone mobile lui-même par son réseau d'abonnement. Cette procédure met en oeuvre dans le cas de la norme GSM un composant électronique spécifique

(carte SIM) branché sur l'appareil, et la possibilité pour le client d'avoir un mot de passe modifiable (code PIN) qui doit être saisi lors de la mise en marche du téléphone.

En cas de vol du téléphone mobile ou du composant SIM, celui-ci peut instantanément être mis hors service pour l'ensemble des réseaux GSM sur un simple appel au fournisseur d'abonnement du téléphone mobile. On pourra prévoir également que suivant une déclaration de vol, l'accès au réseau sera automatiquement fermé.

Le système selon l'invention permet de réutiliser les procédures existantes en ajoutant un niveau de sécurité. Il peut s'appliquer en complément de n'importe quel logiciel d'accès.

Ainsi, la donnée d'identification demandée au client peut être le couple [code d'identification / mot de passe client] (ID/MPC) du protocole d'authentification connu de l'état de la technique, de sorte la connaissance directe ou indirecte de ce couple ne sera plus suffisante en soi pour obtenir l'accès au serveur.

Selon une première variante du système, le site serveur comprend en outre des moyens de génération d'un mot de passe aléatoire ou pseudo-aléatoire, les moyens de synthèse vocale étant adaptés à émettre un message vocal destiné au client via le réseau de téléphonie mobile comprenant ledit mot de passe aléatoire ou pseudo-aléatoire, le mot de passe d'authentification étant dérivé dudit mot de passe aléatoire ou pseudo-aléatoire.

Ce mot de passe d'authentification peut correspondre au mot de passe aléatoire ou pseudo aléatoire transmis par le site serveur via le téléphone ou bien être constitué dudit mot de passe aléatoire auquel est appliqué une clé connue du client et comprise dans la base de données d'authentification du serveur. La clé peut être une constante connue et personnelle par exemple ajoutée ou retranchée pour obtenir le mot de passe serveur. Il peut s'agir aussi d'une opération de logique, comme une permutation.

Selon une seconde variante du système, le site client comporte en outre des moyens de cryptage du mot de passe client selon une clé de cryptage, le mot de passe client crypté obtenu correspond au mot de passe d'authentification et il est transmis au site serveur via le réseau de transmission de données ; et

- les moyens d'authentification du site serveur comportent en outre :
  - des moyens de reconnaissance d'un signal envoyé par le client par les touches du téléphone mobile et correspondant à ladite clé de cryptage ; et
  - des moyens de décryptage du mot de passe client crypté à l'aide de la clé de cryptage reçue via le réseau de téléphonie mobile.

Dans cette seconde variante du système, les touches du téléphone mobile sont utilisées pour transmettre au site serveur la clé de cryptage. Les informations nécessaires au protocole d'authentification sont transmises au site serveur via deux réseaux différents : le mot de passe client crypté par le réseau de transmission de données, par exemple Internet, et la clé de cryptage connue du client via le réseau de téléphonie mobile.

La présente invention propose également un procédé de sécurisation d'accès à un serveur informatique mettant en oeuvre le système selon l'invention, et plus particulièrement la première variante de système, ce procédé comprenant les étapes côté site serveur consistant à :

- demander au client utilisant le site client une donnée d'identification par l'intermédiaire du réseau de transmission de données ;
- rechercher ladite donnée dans une base de données d'authentification;
- rechercher dans la base de donnée d'authentification le numéro de téléphone mobile associé du client ;
- appeler ledit numéro de téléphone mobile ;
- en cas d'obtention de la communication avec le téléphone mobile générer un mot de passe aléatoire ou pseudo-aléatoire ;

- émettre un message vocal comprenant ledit mot de passe aléatoire via le réseau de téléphonie mobile ;

- demander au client de fournir un mot de passe d'authentification dérivé dudit mot de passe aléatoire ou pseudo-aléatoire par l'intermédiaire du réseau de transmission de données ; et

- authentifier ledit mot de passe d'authentification.

La présente invention propose également un procédé de sécurisation d'accès à un serveur informatique mettant en oeuvre le système selon l'invention, et plus particulièrement la seconde variante de système, comprenant les étapes côté site serveur consistant à :

- demander au client une donnée d'identification par l'intermédiaire du réseau de transmission de données ;

- rechercher dans la base de donnée d'authentification le numéro de téléphone mobile associé du client ;

- appeler ledit numéro de téléphone mobile ;

- en cas d'obtention de la communication avec le téléphone mobile, émettre un message vocal demandant la clé de cryptage ;

- authentification du mot de passe d'authentification comprenant :

- la reconnaissance de la clé de cryptage transmise par le client via les touches du téléphone mobile ;

- authentification du mot de passe d'authentification comprenant :

- la reconnaissance de la clé de cryptage transmise par le client via les touches du téléphone mobile ;

- le décryptage du mot de passe d'authentification, correspondant au mot de passe client crypté, à l'aide de ladite clé de cryptage ; et

- l'authentification du mot de passe client ;

ledit procédé comportant côté site client les étapes consistant à crypter le mot de passe client saisi par le client avant de l'envoyer via le réseau de transmission de données.

La connaissance seule ou le vol du contenu de la base de données d'authentification ne suffit pas pour permettre un accès malveillant.

On pourra également renforcer la sécurisation des procédés selon l'invention, en prévoyant la désactivation automatique de l'accès au serveur dès qu'un nombre prédéterminé de tentatives a échoué à l'une quelconque des étapes de saisie, et la possibilité de demander la désactivation immédiate du téléphone auprès du fournisseur de téléphonie mobile.

La présente invention sera mieux comprise et d'autres avantages apparaîtront à la lumière de la description qui va suivre de deux exemples de réalisation du système et des procédés associés selon l'invention, description faite en référence aux dessins annexés sur lesquels :

- la figure 1 est un schéma synoptique du premier exemple de réalisation du système selon l'invention ;

- la figure 2 est un organigramme du procédé d'authentification exécuté par le serveur mettant en oeuvre le système de la figure 1 ;

- la figure 3 montre schématiquement une page écran générée par le serveur et utilisée par le client pour la transaction d'authentification du procédé de la figure 2 ;

- la figure 4 est un schéma synoptique du second exemple de réalisation du système selon l'invention ;

- la figure 5 est un organigramme du procédé d'authentification exécuté par le serveur mettant en oeuvre le système de la figure 4 ; et

- la figure 6 montre schématiquement une page écran générée par le serveur et utilisée par le client pour la transaction d'authentification du procédé de la figure 5 ;

Comme illustré schématiquement à la figure 1, un premier exemple de réalisation du système selon l'invention comprend :

- sur un site client 1, un ordinateur individuel 2 équipé d'un modem 3 pour accéder à un réseau de transmission de données 4 et

un téléphone mobile 5 personnel, abonné à un réseau de téléphonie mobile 6, par exemple au standard GSM ; et

- sur un site serveur 7, un serveur constitué d'un ordinateur 8 sur lequel est chargé un logiciel adapté à gérer le procédé d'accès du client aux services 9 du serveur selon l'invention, notamment le protocole d'authentification du client ; l'ordinateur est équipé d'un modem 10 lui permettant d'établir une liaison avec le réseau de téléphonie mobile 6 et d'appeler un numéro de téléphone, de moyens 11 de génération d'un mot de passe aléatoire ou pseudo-aléatoire MPA, et d'un circuit de synthèse vocale 12 lui permettant de communiquer au téléphone mobile 5 un message comprenant le mot de passe MPA généré aléatoirement nécessaire au protocole d'authentification. L'ordinateur 8 est relié à une base de données d'authentification BDA comprenant pour chaque client répertorié un triplet [code d'identification ID / mot de passe client MPC/numéro de téléphone mobile personnel associé].

Le procédé d'accès sécurisé se déroule de la manière suivante.

Le client sur le site client 1 demande l'accès au serveur. La liaison entre le site client 1 et le site serveur 7 via le réseau de transmission de données 4 se fait de manière classique et connue en soi par l'intermédiaire du modem 3 du site client 1, du réseau téléphonique commuté, d'un fournisseur d'accès au réseau généraliste Internet et d'Internet.

En retour, le serveur affiche sur l'ordinateur individuel 2 une page écran 15, représentée sur la figure 3, comprenant trois champs de saisie : les deux premiers champs 16 et 17 correspondent au couple classique [code d'identification ID et mot de passe client MPC], le troisième champs 18 correspond à un mot de passe d'authentification MPAUT qui est dérivé du mot de passe aléatoire ou pseudo-aléatoire MPA qui sera communiqué par le serveur au site client 1 via le téléphone mobile 5. Ce mot de passe d'authentification MPAUT

correspond ici au mot de passe aléatoire ou pseudo-aléatoire MPA généré par le serveur.

Dans un premier temps, le client saisit son couple [code d'identification-mot de passe client] (ID/MPC) qui est déjà sécurisé par n'importe quel processus connu à partir de la base de données d'authentification BDA.

En se référant à l'organigramme de la figure 2, les étapes suivantes du protocole, spécifiques à la présente invention, ne seront exécutées par le serveur qu'à la condition préalable que l'étape de contrôle identification / mot de passe client à l'étape 20 soit couronnée de succès.

Si tel est le cas, l'étape suivante 21 consiste à composer le numéro du téléphone mobile identifié grâce à la base de données d'authentification BDA à l'aide du modem 10. A l'étape suivante 22, si la communication téléphonique avec le téléphone mobile est obtenue (par exemple par l'indication du " décrochage " par le modem 10 du site serveur), le serveur génère un mot de passe aléatoire MPA et émet grâce à son circuit de synthèse vocale ce mot de passe MPA généré vers le téléphone mobile 5. L'étape suivante 23 correspond à une étape d'attente de la saisie du mot de passe d'authentification MPAUT par le client au niveau du site client pendant une durée limitée prédéterminée (étape 24). Si à l'étape 25, le mot de passe MPAUT saisi est conforme, l'authentification est confirmée et le client peut accéder aux services 9 du serveur.

L'échec de l'authentification intervient donc dans les circonstances suivantes :

- échec de l'authentification classique du couple [ID /MPC] ;
- non-obtention de la communication avec le téléphone mobile ;
- mauvaise ou absence d'entrée du second mot de passe MPAUT dans le délai prédéterminé.

Des variantes de réalisation sont possibles, notamment concernant le mot de passe serveur dérivé du mot de passe aléatoire

MPA qui peut être constitué dudit mot de passe aléatoire MPA auquel est ajoutée une clé arithmétique ou logique personnelle au client et comprise dans la base de données d'authentification BDA dans un champs supplémentaire à ceux déjà prévus pour le code d'identification ID, le mot de passe client MPC et le numéro de téléphone mobile. Le serveur sera équipé de moyens lui permettant de recalculer le mot de passe généré MPA pour procéder à l'étape d'authentification.

Les figures 4 à 6 concernent un autre mode de réalisation du système selon l'invention se différenciant par le fait que le site client 1 est équipé en outre de moyens de cryptage 30 qui sont adaptés à crypter le mot de passe client MPC une fois celui-ci saisi par le client avant de l'envoyer via le réseau 4 de transmission de données au site serveur 7. Du côté du site serveur, celui se différencie par des moyens de reconnaissance 31 d'un signal envoyé par le client via les touches de son téléphone mobile personnel 5 et des moyens de décryptage 32 adaptés à décrypter le mot de passe client MPC selon une clé de cryptage qui est transmise par le client via les touches de son téléphone mobile. La base de données d'authentification BDA ne comporte ici que deux champs contenant l'un le code ID et l'autre le mot de passe client MPC. Le protocole d'authentification après décryptage correspond au protocole connu dans l'art antérieur.

Le procédé d'accès sécurisé utilisant ce système se déroule de la manière suivante.

En réponse à une demande d'accès de la part du client utilisant le site client 1, le serveur affiche sur l'ordinateur individuel 2 une page écran 35 représentée à la figure 6, ne comprenant par rapport au premier mode de réalisation que deux champs de saisie 36 et 37 qui correspondent au couple classique [code d'identification ID et mot de passe client MPC]. Immédiatement après la saisie du mot de passe client MPC, les moyens 30 cryptent le mot de passe client saisi selon une clé de cryptage connue seulement du client. Ce mot de passe

client crypté correspond au mot de passe dit d'authentification du procédé selon l'invention.

En se référant à l'organigramme de la figure 5, les étapes du protocole d'authentification se déroulent de la manière suivante.

Dans un premier temps, à l'étape 40, le serveur, ayant reçu le mot de passe client crypté et le code ID, identifie le client à l'aide du code d'identification ID, puis à l'étape 41, il recherche dans la base de données d'authentification BDA, le numéro de téléphone mobile. L'étape 42 suivante consiste à composer le numéro du téléphone mobile à l'aide du modem 10. Si à l'étape suivante 43 la communication avec le téléphone mobile est obtenue, le serveur émet grâce à son circuit de synthèse vocale 12 un message (étape 45) signalant qu'il attend de la part du client la clé de cryptage via les touches du téléphone mobile. L'étape 46 correspond à une étape d'attente de la saisie de cette clé pendant une durée limitée prédéterminée. L'étape suivante 47 consiste à authentifier le mot de passe MPAUT reçu via le réseau 4 par le décryptage de ce mot de passe avec la clé et l'authentification du mot de passe client obtenu, conformément au protocole d'authentification. Si le mot de passe client MPC est conforme (étape 48), l'authentification est confirmée et le client peut accéder aux services 9 offert par le serveur.

L'échec de l'authentification interviendra donc dans les circonstances suivantes :

- non-obtention de la communication avec le téléphone mobile ; et
- mauvaise ou absence d'entrée du mot de passe client MPC et de la clé de cryptage.

Revendications

1. Système d'accès sécurisé à un serveur informatique, comportant:

- un site client (1) comprenant des moyens d'accès (3) à un réseau de transmission de données (4) et une unité centrale de contrôle et de traitement de données (2) ; et
- un site serveur (7) comprenant des moyens d'accès audit réseau de transmission de données et une unité centrale de commande et de traitement de données (8) prévue notamment pour gérer un protocole d'authentification du client utilisateur du site client,

caractérisé en ce que :

- le site client (1) comprend en outre un téléphone mobile (5) ; et
- le site serveur (7) comprend en outre :
- des moyens de connexion (10) au réseau de téléphonie mobile (6) dudit téléphone mobile et d'appel d'un numéro de téléphone ;
- une base de données d'authentification (BDA) comprenant une donnée d'identification (ID/MPC) du client et un numéro de téléphone mobile associé ;
- des moyens de synthèse vocale ; et
- des moyens d'authentification d'un mot de passe d'authentification (MPAU) reçu par le site serveur via le réseau de transmission de données (4).

2. Système selon la revendication 1 caractérisé en outre en ce que le site serveur comprend des moyens de génération d'un mot de passe aléatoire ou pseudo-aléatoire (MPA), les moyens de synthèse vocale étant adaptés à émettre un message vocal destiné au client via le réseau de téléphonie mobile comprenant ledit mot de passe aléatoire ou pseudo-aléatoire, le mot de passe d'authentification (MPAU) étant dérivé dudit mot de passe aléatoire ou pseudo-aléatoire (MPA).

3. Système selon la revendication 2, caractérisé en ce que le mot de passe d'authentification (MPAU) correspond au mot de passe aléatoire ou pseudo-aléatoire (MPA) généré par le serveur et communiqué via le téléphone mobile.

4. Système selon la revendication 2 ou 3, caractérisé en ce que le mot de passe d'authentification (MPAU) est constitué par le mot de passe aléatoire ou pseudo-aléatoire (MPA) généré par le serveur et communiqué via le téléphone mobile auquel est appliquée une clé connue du client et comprise dans la base de donnée d'authentification (BDA) du serveur.

5. Système selon l'une des revendications 2 à 4, caractérisé par des moyens de contrôle de la donnée d'identification.

6. Système selon la revendication 5, caractérisé en ce que la donnée d'identification est constituée par un couple [code d'identification / mot de passe client] (ID,MPC) compris dans la base de donnée d'authentification du serveur.

7. Système selon l'une des revendications 2 à 6, caractérisé en ce qu'il comporte des moyens de temporisation pour limiter dans le temps la possibilité de transmission pour le site client du mot de passe d'authentification (MPAU).

8. Système selon la revendication 6 ou 7, caractérisé en ce que la base de données d'authentification (BDA) comprend pour chaque client quatre champs :

- un champs comprenant le code d'identification (ID) ;
- un champs comprenant le mot de passe client (MPC) ;

- un champs comprenant le numéro de téléphone mobile du client ; et
- un champs comprenant la clé.

9. Système selon la revendication 1, caractérisé en ce que :
- le site client comporte des moyens de cryptage du mot de passe client (MPC) selon une clé de cryptage, le mot de passe client crypté obtenu correspond au mot de passe d'authentification (MPAUT) et il est transmis au site serveur via le réseau de transmission de données (4) ; et
- les moyens d'authentification du site serveur comportent en outre :
  - des moyens de reconnaissance d'un signal envoyé par le client par les touches du téléphone mobile et correspondant à ladite clé de cryptage ; et
  - des moyens de décryptage du mot de passe client crypté à l'aide de la clé de cryptage reçue via le réseau de téléphonie mobile (6).

10. Système selon la revendication 9, caractérisé en ce qu'il comporte des moyens de temporisation pour limiter dans le temps la possibilité de transmission pour le client de la clé de cryptage via les touches du téléphone mobile.

11. Procédé de sécurisation d'accès à un serveur informatique (7), mettant en oeuvre un système selon l'une des revendications 1 à 8, comprenant les étapes côté site serveur consistant à :
- demander au site client une donnée d'identification (ID,MPC) par l'intermédiaire du réseau de transmission de données (4) ;
- rechercher ladite donnée (ID,MPC) dans une base de données d'authentification (BDA) ;
- rechercher dans la base de donnée d'authentification (BDA) le numéro de téléphone mobile associé du client ;

- appeler ledit numéro de téléphone mobile ;
- en cas d'obtention de la communication avec le téléphone mobile générer un mot de passe aléatoire ou pseudo-aléatoire (MPA) ;
- émettre un message vocal comprenant ledit mot de passe aléatoire (MPA) via le réseau de téléphonie mobile (6) ;
- demander au client de fournir un mot de passe d'authentification (MPAUT) dérivé dudit mot de passe aléatoire ou pseudo-aléatoire (MPA) par l'intermédiaire du réseau de transmission de données (4) ; et
- authentifier ledit mot de passe d'authentification (MPAUT).

12. Procédé selon la revendication 11, caractérisé en ce que le mot de passe d'authentification (MPAUT) correspond au mot de passe aléatoire ou pseudo-aléatoire (MPA) généré par le serveur et communiqué via le téléphone mobile.

13. Procédé selon la revendication 11, caractérisé en ce que le mot de passe d'authentification (MPAUT) est constitué par le mot de passe aléatoire ou pseudo-aléatoire (MPA) généré par le serveur et communiqué via le téléphone mobile, auquel est appliquée une clé connue du client et comprise dans la base de donnée d'authentification du serveur (BDA), l'étape d'authentification comportant une étape de conversion dudit mot de passe d'authentification en mot de passe aléatoire ou pseudo-aléatoire (MPA) par application de ladite clé.

14. Procédé selon l'une quelconque des revendications 11 à 13, caractérisé par une étape de contrôle de la donnée d'identification (ID,MPC) préalable à l'appel du numéro de téléphone mobile.

15. Procédé selon la revendication 14, caractérisé en ce que la donnée d'identification demandée au client est un couple [code d'identification / mot de passe client] (ID/MPC).

16. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape qui consiste à demander au client le mot de passe d'authentification (MPAUT) se déroule pendant une durée prédéterminée au delà de laquelle l'authentification est refusée.

17. Procédé de sécurisation d'accès à un serveur informatique (7), mettant en oeuvre un système selon l'une des revendications 1, 9 ou 10, comprenant les étapes côté site serveur consistant à :

- demander au client une donnée d'identification (ID) par l'intermédiaire du réseau de transmission de données (4) ;
- rechercher dans la base de donnée d'authentification (BDA) le numéro de téléphone mobile associé du client ;
- appeler ledit numéro de téléphone mobile ;
- en cas d'obtention de la communication avec le téléphone mobile, émettre un message vocal demandant la clé de cryptage ;
- authentification du mot de passe d'authentification (MPAUT) comprenant :
  - la reconnaissance de la clé de cryptage transmise par le client via les touches du téléphone mobile ;
  - le décryptage du mot de passe d'authentification (MPAUT), correspondant au mot de passe client crypté, à l'aide de ladite clé de cryptage ; et
  - l'authentification du mot de passe client (MPC) ;

ledit procédé comportant côté site client les étapes consistant à crypter le mot de passe client (MPC) saisi par le client avant de l'envoyer via le réseau de transmission de données (4).

18. Procédé selon la revendication 17, caractérisé en ce que l'étape qui consiste à réceptionner le signal représentatif de la clé de cryptage se déroule pendant une durée prédéterminée au delà de laquelle l'authentification est refusée.

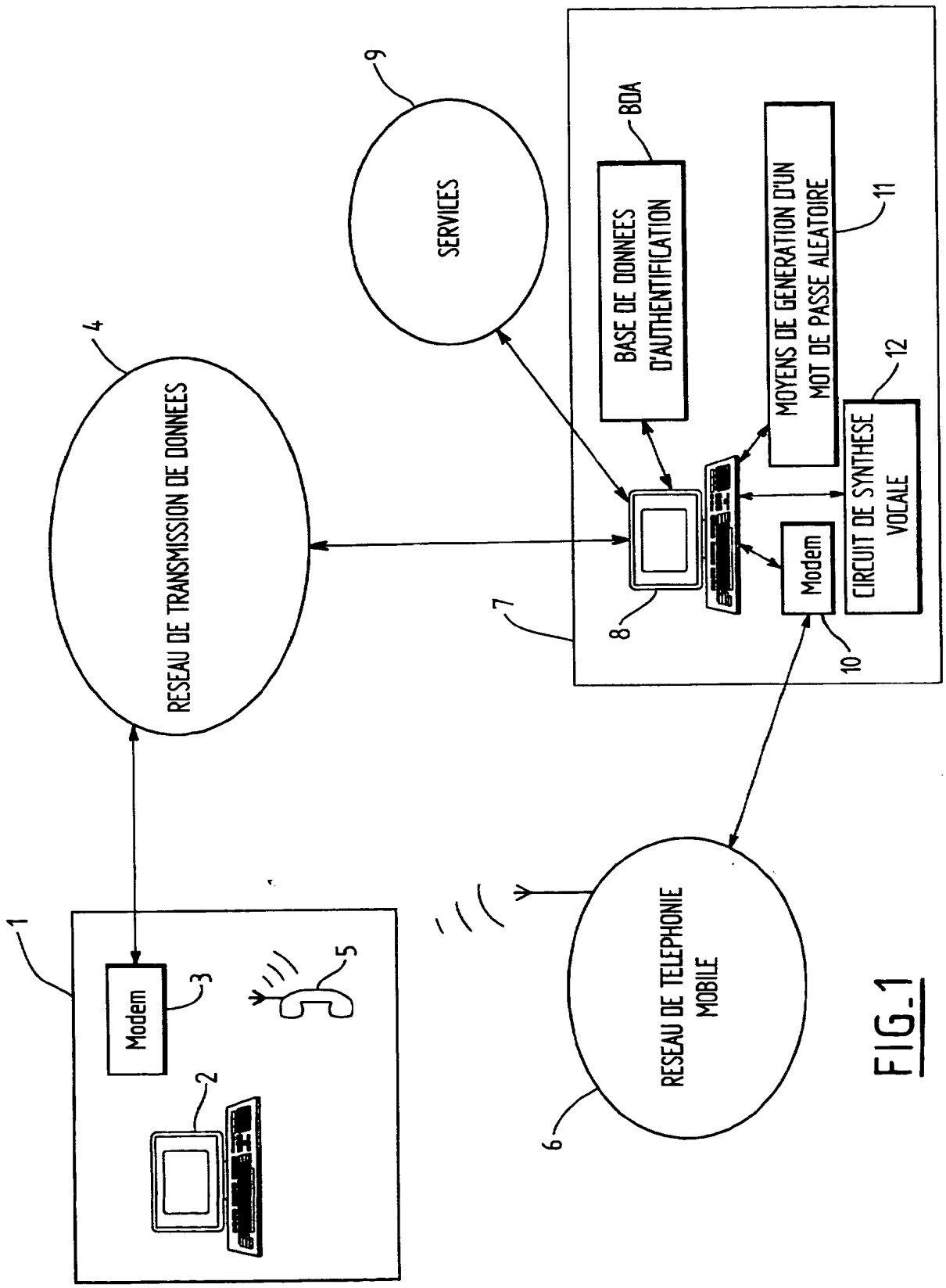
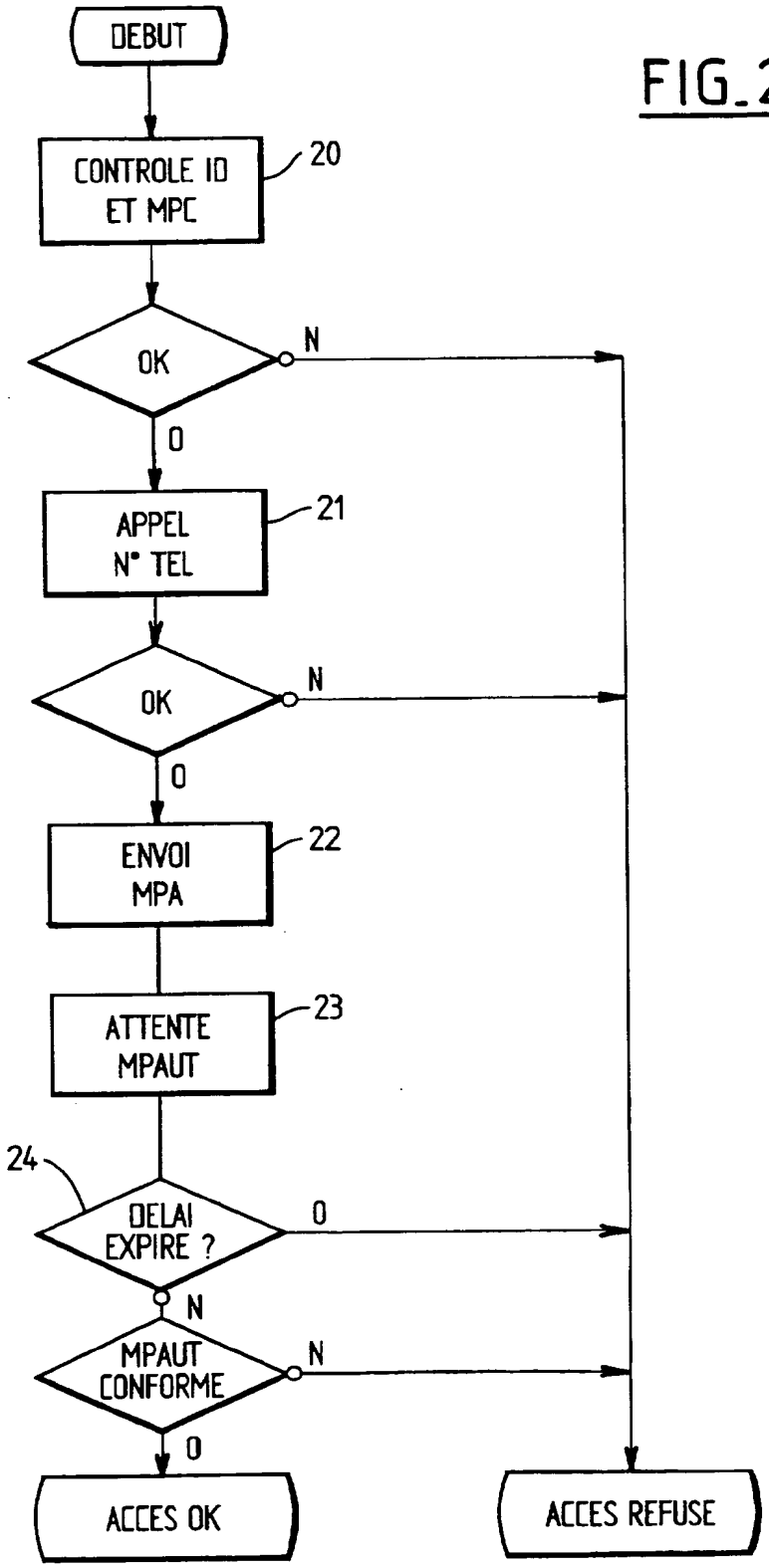


FIG.1

FIG_2



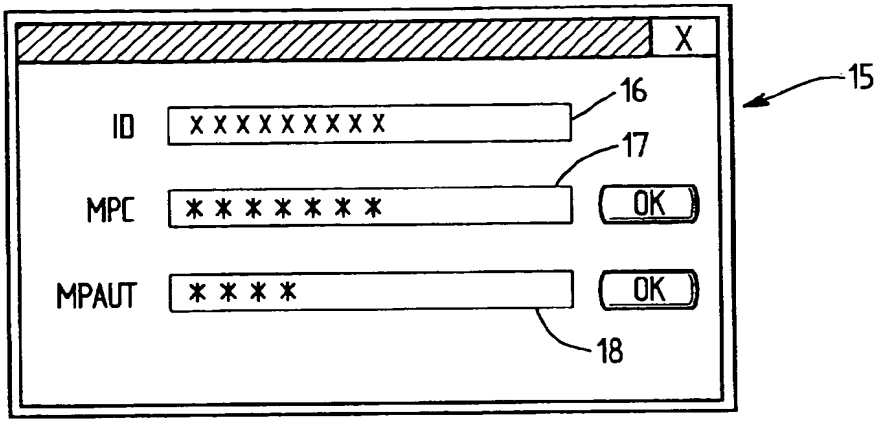


FIG_3

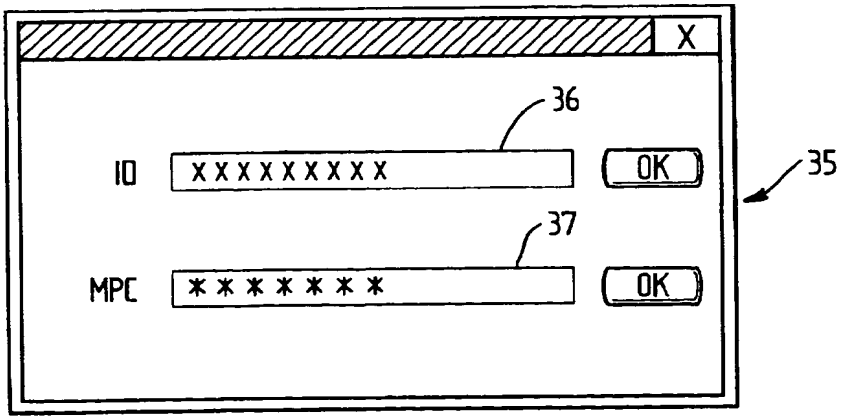


FIG_6

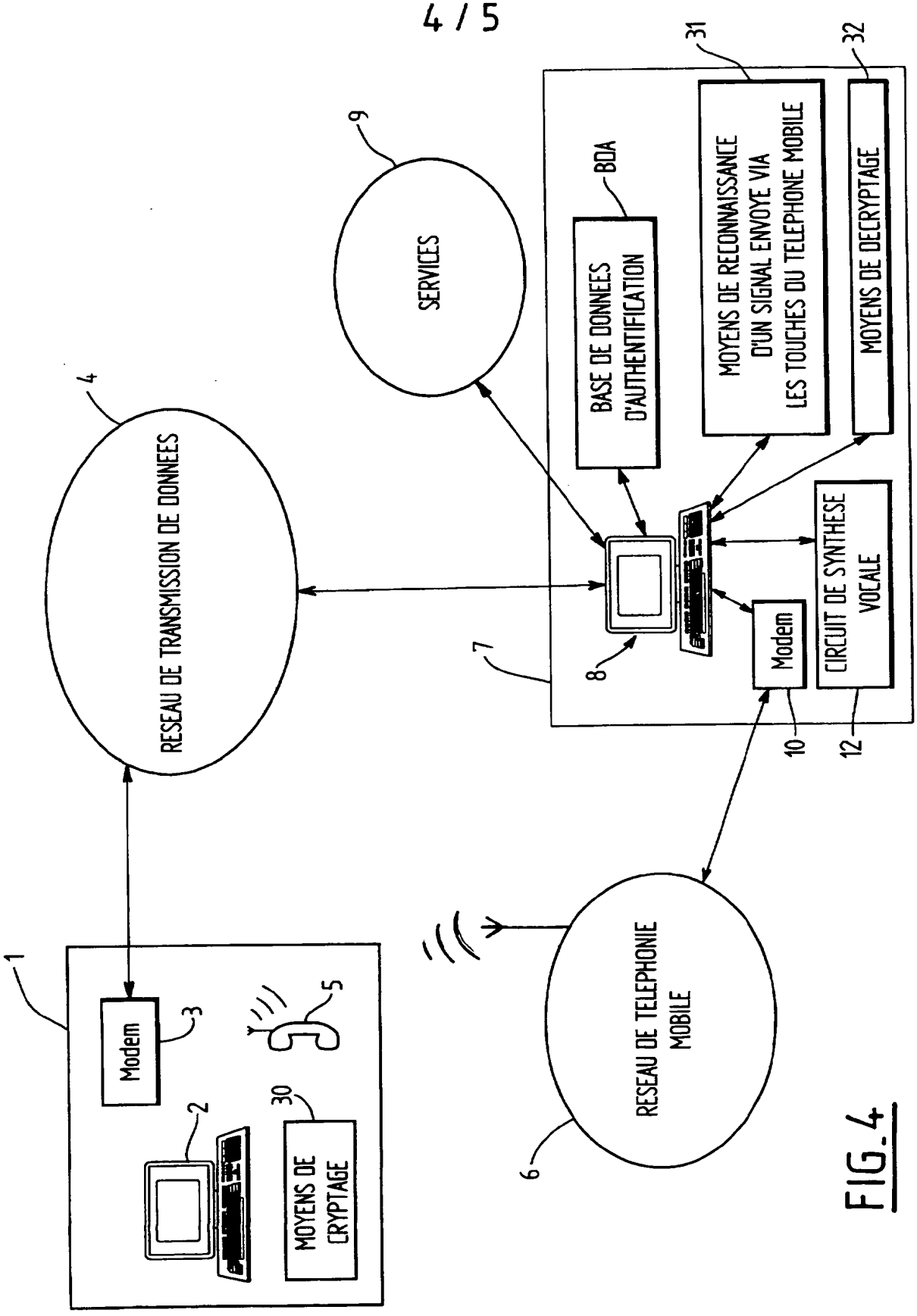


FIG.4

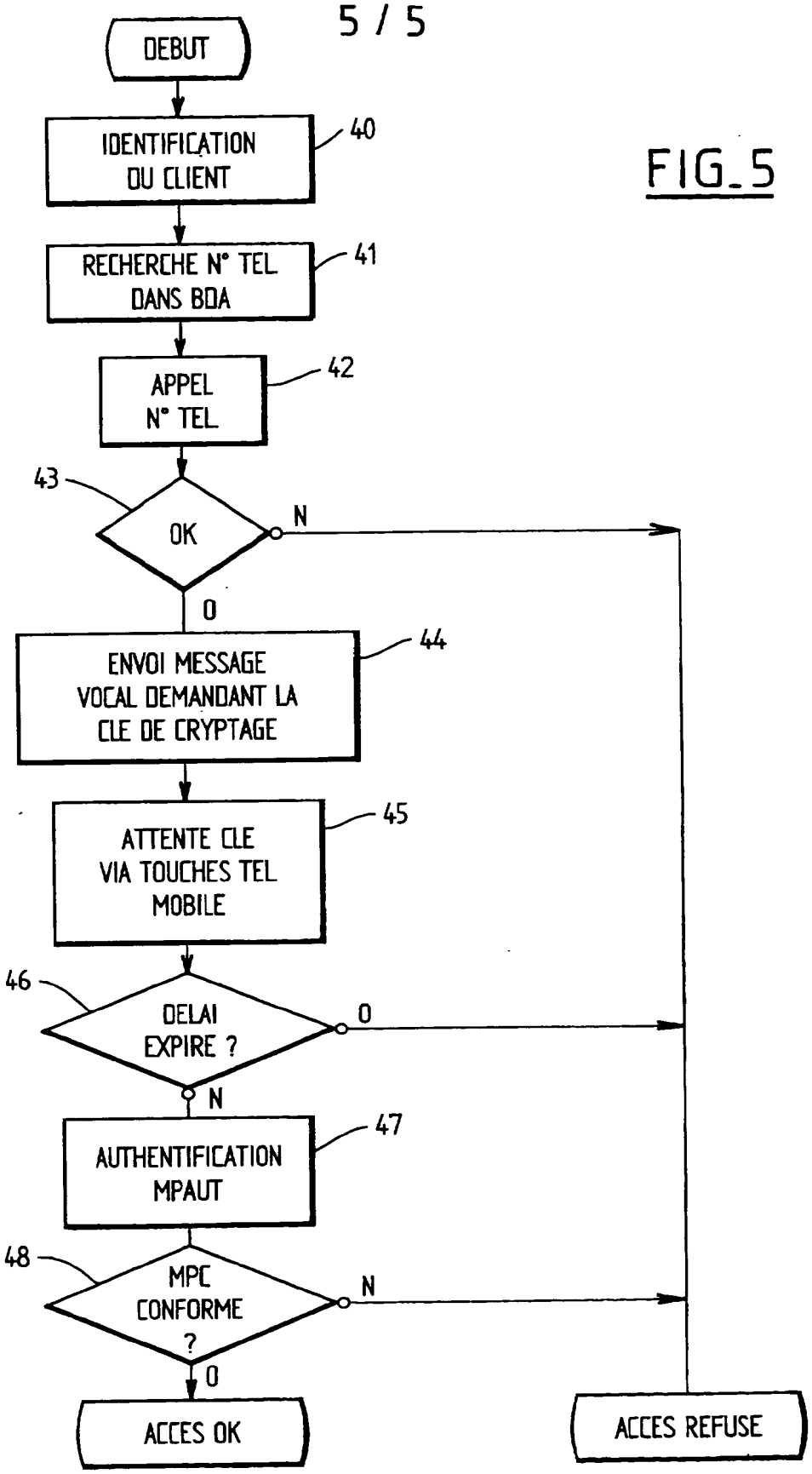


FIG_5

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2795264

N° d'enregistrement national

FA 579523
FR 9907613

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	WO 97 31306 A (NOKIA MOBILE PHONES LTD ;KURKI TEEMU (FI); SORMUNEN TONI (FI)) 28 août 1997 (1997-08-28)	1,9
A	* page 3, ligne 11 - page 4, ligne 33 * * page 5, ligne 35 - page 7, ligne 23 * * page 8, ligne 5-22 * * page 9, ligne 13-24 * * figure 2 *	2-8, 10-18
A	DE 197 24 901 A (SIEMENS NIXDORF INF SYST) 17 décembre 1998 (1998-12-17) * colonne 1, ligne 63 - colonne 2, ligne 27 * * colonne 2, ligne 37 - colonne 3, ligne 32 * * colonne 3, ligne 54 - colonne 4, ligne 39 *	1-18
A	EP 0 818 915 A (AT & T CORP) 14 janvier 1998 (1998-01-14) * colonne 1, ligne 40 - colonne 2, ligne 51 * * colonne 3, ligne 32 - colonne 5, ligne 9 * * colonne 5, ligne 40 - colonne 6, ligne 23 *	1-18

DOMAINES TECHNIQUES RECHERCHES (Int.CL.7)
H04L
G06F
H04Q

Date d'achèvement de la recherche: 26 mai 2000

Examinateur: Lázaro Lõpez, M.L.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1

EPO FORM 1503 03.82 (P04C19)